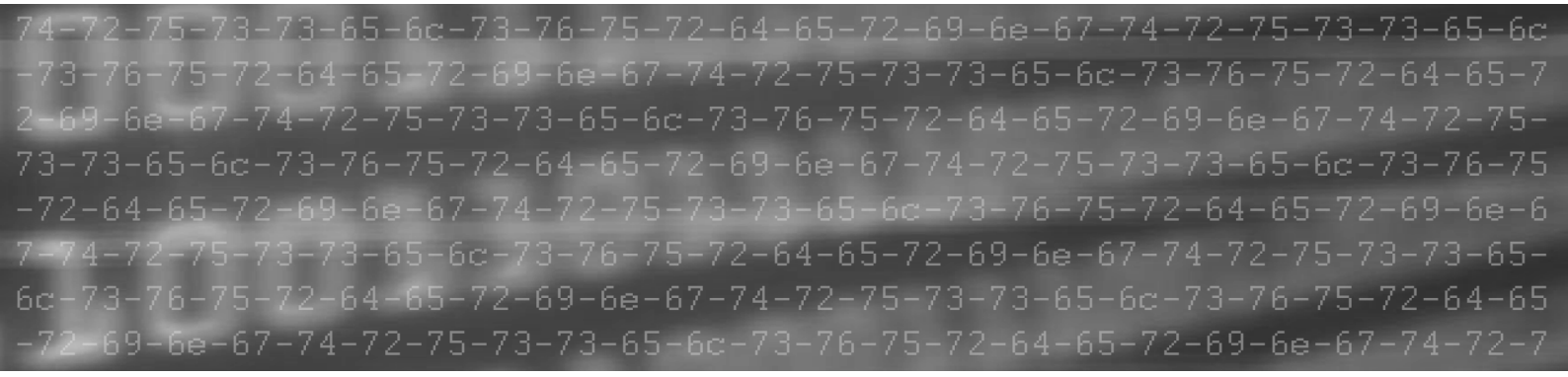
CENTRE FOR
CYBER SECURITY

Threat Assessment

Destructive cyberattacks may hit Danish companies and public authorities



Threat Assessment Branch under the Centre for Cyber Security

July 2017

CENTRE FOR
CYBER SECURITY

6 July 2017

Threat assessment: Destructive cyberattacks may hit Danish companies and public authorities

Key Assessment

- Danish companies and public authorities may be hit by destructive cyberattacks from foreign states or organized hacker groups, especially companies located or operating in conflict areas where the risk of destructive cyberattacks is increased.
- Foreign states likely launch destructive cyberattacks disguised as other types of attacks such as ransomware attacks.
- It is less likely that foreign states with destructive cyberattack capabilities will direct an actual destructive cyberattack against an industrial system or critical infrastructure in Denmark.

Analysis

The Danish Defence Intelligence Service's Centre for Cyber Security (CFCS) assesses that Danish companies and public authorities may become targets of destructive cyberattacks from foreign states or organized hacker groups, especially organizations operating in conflict areas where there is an increased risk of destructive cyberattacks or in areas that have previously been exposed to destructive cyberattacks. In such areas, the organizations could become collateral damage in connection with destructive cyberattacks against other targets, or they could be sub-targets in connection with large-scale, full-spectrum cyber campaigns in the area.

CFCS's general threat assessment has previously outlined how foreign states have launched cyberattacks against industrial systems abroad. Companies that cooperate with local partners or are otherwise present in conflict areas or areas where foreign states with strong cyber capabilities have vested interests – for example in some parts of the Middle East such as the GCC countries, South Korea in Asia and parts of Eastern Europe such as Ukraine – should be aware of the threat from hackers with destructive cyberattack capabilities.

CFCS assesses it likely that hacker groups launch destructive cyberattacks disguised as other types of attacks, for instance financial crime. It is likely that the NotPetya campaign, which o 27 June 2017 affected several international companies, including Danish companies, was an example of

such an attack. Preliminary investigations into the malware used in the campaign and the absence of the possibility to pay ransom indicate that NotPetya was a destructive cyberattack disguised as a ransomware attack.

If so, the 27 June 2017 NotPetya attack was one of the largest destructive cyberattacks ever seen in Europe, suggesting that hackers are becoming increasingly ready to use this tool.

However, CFCS still assesses it less likely that foreign states with destructive cyber capabilities will launch an actual destructive cyberattack against an industrial system or critical infrastructure in Denmark. Nevertheless, this situation could change in the event of a political or military conflict between Denmark and a foreign state with destructive cyber capabilities.

A destructive cyberattack is a multi-purpose tool that can be used by various actors. The desired effect of a cyberattack determines whether or not it can be categorized as destructive. We define a destructive cyberattack as a cyberattack aimed at causing injury or death to persons; significant damage or destruction to objects; serious financial consequences; or destruction or manipulation of information, data or software that renders them unfit for use.

Recommendations

Based on the concrete threat, we have prepared the following cyber defence recommendations which organizations should take into account in their work with risk assessments and implementation of specific countermeasures.

- CFCS recommends that the senior management ensures that the specific threat is addressed by in-house risk assessments. This requires an overview of business processes, IT infrastructure and IT processes as well as identification of vulnerabilities.
- Network segmentation and segregation should reflect the organization's different physical locations. Segmentation means that a network is split into smaller subnetworks/segments. In each of the subnetworks/segments, a set of rules should be implemented defining the individual IT units' authorization to communicate with other IT units in the infrastructure.
- User rights and administrator rights should be on a strict 'need-to-use' basis, and system passwords and other passwords should be different from segment to segment.
- Organizations should systematically back up critical information, key configuration files and other types of setup data. They should establish a regular backup routine and regularly ensure that backup restoration functions as intended as well as decide where to store backup data. Off-line backup is a good idea as it diminishes vulnerability to the threat described above.
- Follow the recommendations in the May 2017 'WannaCry Ransomware attack – removal of malware'. Be aware of vulnerabilities in some SMB versions. In the CFCS guideline 'Cyber defence that works', a specific and prioritised plan on how to reduce the risk of a cyberattack and how to address its most serious repercussions is described. In this guideline, it is emphasized that patching is crucial in connection with the specific threat and could significantly reduce the risk.

- Well-tested plans for restoration following a system breakdown could help an organization under attack to implement the necessary and required countermeasures and return to business as usual as quickly as possible.
- In order for the organization to identify and react to deviations from the normal picture, regular monitoring and logging of relevant networks and systems should be carried out. See the CFCS guideline 'Logging – a key element in good cyber defence practice' for more information on the subject.
- The cyber threat is very dynamic and constantly evolving. Consequently, organizations should follow political developments in the area where they operate and be prepared to adjust their networks and security to new threats.

Below is the scale of probability the DDIS applies